PCT/DE 98/00563

BUNDESREPUBLIK DEUTSCHLAND

09/402144

Bescheinigung

Die Siemens Aktiengesellschaft in München/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren und Anordnung zur Bildung und Überprüfung einer Prüfsumme für digitale Daten, die in mehrere Datensegmente gruppiert sind"

am 14. April 1997 beim Deutschen Patentamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patentamt vorläufig die Symbole H 04 L und G 06 F der Internationalen Patentklassifikation erhalten.

München, den 12. Februar 1998

Der Präsident des Deutschen Patentamts

Im Auftrag

Nietiedt

Aktenzeichen: 197 15 486.7

A 9161-8
(EVA-L)
04/94

Beschreibung

Verfahren und Anordnung zur Bildung und Überprüfung einer Prüfsumme für digitale Daten, die in mehreren Datensegmente gruppiert sind

Bei der digitalen Kommunikation, d.h. beim Austausch digitaler Daten ist es oftmals wünschenswert, die Übertragung der elektronischen Daten hinsichtlich verschiedenster Aspekte abzusichern.

Ein sehr bedeutender Aspekt ist der Schutz der zu übertragenden digitalen Daten gegen unerlaubte Modifikation, die sog. Sicherung der Integrität der Daten.

Aus [1] ist zum Schutz gegen unerlaubte Modifikation digitaler Daten die sog. kryptographische Prüfsumme bekannt, z.B. die digitale Signatur. Das in [1] beschriebene Verfahren basiert auf der Bildung eines Hashwertes aus den digitalen Nutzdaten und der anschließenden kryptographischen Bearbeitung des Hashwertes mit einem kryptographischen Schlüssel. Das Ergebnis ist eine kryptographische Prüfsumme. Zur Überprüfung der Integrität wird mit einem entsprechenden kryptographischen Schlüssel die inverse kryptographische Operation auf die gebildete Prüfsumme durchgeführt und das Ergebnis mit dem erneut aus den Nutzdaten berechneten Hashwert verglichen. Bei Übereinstimmung der ermittelten Hashwerte ist die Integrität der Nutzdaten gewährleistet.

Diese bisher übliche Vorgehensweise bedingt, daß die kompletten Nutzdaten auf Empfängerseite in identischer Reihenfolge, wie sie bei der Bildung des Hashwertes vorlagen, vorliegen müssen, da sonst die Hashwertbildung zu einem fehlerhaften Wert führt. Oftmals ist es jedoch bei der digitalen Kommunikation üblich, die zu übertragenden Nutzdaten aufgrund von Protokollrandbedingungen in kleinere Datensegmente, die auch als Datenpakete bezeichnet werden, zu unterteilen und zu

Datensegment eine erste Segmentprüfsumme gebildet. Die gebildeten ersten Segmentprüfsummen werden durch eine kommutative Verknüpfung zu einer ersten kommutativen Prüfsumme verknüpft.

Bei dem Verfahren gemäß Patentanspruch 2 wird eine vorgegebene erste kommutative Prüfsumme, die digitalen Daten zugeordnet ist, die in mehrere Datensegmente gruppiert sind, überprüft. Dies erfolgt dadurch, daß für jedes Datensegment eine zweite Segmentprüfsumme gebildet wird und durch eine kommutative Verknüpfung der zweiten Segmentprüfsummen eine zweite kommutative Prüfsumme gebildet wird. Die zweite kommutative Prüfsumme und die erste kommutative Prüfsumme werden auf Übereinstimmung überprüft.

Bei dem Verfahren gemäß Patentanspruch 3 zur Bildung und Überprüfung einer ersten kommutativen Prüfsumme für digitale Daten, die in Datensegmente gruppiert sind, wird für jedes Datensegment eine erste Segmentprüfsumme gebildet und die ersten Segmentprüfsummen werden durch eine kommutative Verknüpfung zu einer ersten kommutativen Prüfsumme verknüpft. Für jedes Datensegment der digitalen Daten, denen die erste kommutative Prüfsumme zugeordnet ist, werden zweite Segmentprüfsummen gebildet und durch kommutative Verknüpfung der zweiten Segmentprüfsummen wird eine zweite kommutative Prüfsumme gebildet. Die zweite kommutative Prüfsumme und die erste kommutative Prüfsumme werden auf Übereinstimmung überprüft.

Die Anordnung gemäß Patentanspruch 11 weist eine Recheneinheit auf, die derart eingerichtet ist, daß für jedes Datensegment eine Segmentprüfsumme gebildet wird, und daß durch eine kommutative Verknüpfung der Segmentprüfsummen die erste kommutative Prüfsumme gebildet wird.

Die Anordnung gemäß Patentanspruch 12 weist eine Recheneinheit auf, die derart eingerichtet ist, daß für jedes Datensegment eine zweite Segmentprüfsumme gebildet wird, durch eine kommutative Verknüpfung der zweiten Segmentprüfsummen eine

bei der Bildung der ersten Prüfsumme beizubehalten. Dies führt zu einer Zeitersparnis bei der Überprüfung der Integrität der Daten.

Anschaulich kann die Erfindung darin gesehen werden, daß bei mehreren Datensegmenten, die insgesamt die zu schützenden Daten darstellen, für jedes Datensegment eine Prüfsumme gebildet wird und die einzelnen Prüfsummen der Datensegmente kommutativ miteinander verknüpft werden.

Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Es ist vorteilhaft, die erste kommutative Prüfsumme unter Verwendung mindestens einer kryptographischen Operation kryptographisch abzusichern.

Durch diese Weiterbildung wird erreicht, daß die kryptographische Sicherheit der Daten erheblich erhöht wird. Eine kryptographische Operation in diesem Sinne ist beispielsweise die Verschlüsselung der ersten kommutativen Prüfsumme mit einem symmetrischen oder auch mit einem asymmetrischen Verschlüsselungsverfahren, wodurch eine kryptographische Prüfsumme gebildet wird. Auf Empfängerseite wird das inverse kryptographische Verfahren zu dem kryptographischen Verfahren durchgeführt, um die kryptographische Sicherheit zu gewährleisten.

Zur Bildung einer Prüfsumme, wie sie im Rahmen des Dokuments zu verstehen ist, sind verschiedene Möglichkeiten bekannt:
-eine Prüfsumme kann durch Bildung von Hashwerten für die einzelnen Datensegmente gebildet werden;
- die Prüfsummen können auch durch sog. zyklische Codes (Cyclic Redundancy Check, CRC) gebildet werden;
- es kann ferner eine kryptographische Einwegfunktion zur Bildung der Prüfsummen für die Datensegmente verwendet werden.

len Daten, die auch als Nutzdaten bezeichnet werden, für die es gilt, die Integrität zu gewährleisten.

Sowohl die erste Rechneranordnung A1 als auch eine im weiteren beschriebene zweite Rechneranordnung A2 enthalten jeweils eine Recheneinheit R, die derart eingerichtet ist, daß die im weiteren beschriebenen Verfahrensschritte durchgeführt werden.

In der ersten Anordnung A1 sind die Datensegmente Di an Positionen Pi innerhalb des gesamten Datenstroms angeordnet. Für jedes Datensegment Di wird eine erste Segmentprüfsumme PSi unter Verwendung einer Prüfsummenfunktion PSF. Die einzelnen ersten Segmentprüfsumme PSi werden durch eine kommutative Verknüpfung, wie sie in [2] definiert und beschrieben ist, zu einer ersten kommutativen Prüfsumme KP1 verknüpft. Die kommutative Verknüpfung zwischen den einzelnen Prüfsummen PSi sind in der Figur durch ein EXOR-Zeichen $\oplus$ symbolisch dargestellt.

Die erste kommutative Prüfsumme KP1 wird einem kryptographischen Verfahren, einem symmetrischen oder asymmetrischen Verfahren, unter Verwendung eines ersten kryptographischen Schlüssels S unterzogen (Schritt 101). Das Ergebnis der kryptographischen Operation ist eine kryptographische Prüfsumme KP.

Sowohl die Datensegmente Di als auch die kryptographische Prüfsumme KP werden über ein Übertragungsmedium, vorzugsweise eine Leitung oder auch eine logischen Verbindung, die in der Fig. durch eine Kommunikationsverbindung UM symbolisch dargestellt ist, zu einer zweiten Anordnung A2 übertragen und dort empfangen.

Die sich überkreuzenden Pfeile der Datensegmente Di in der Figur deuten an, daß durch die Übertragung der Datensegmente Di diese in einer gegenüber der Reihenfolge in der ersten An-

Ist dies der Fall, so ist die Integrität der Datensegmente Di und somit die Integrität der gesamten digitalen Daten gewährleistet (Schritt 104), wenn die verwendeten kryptographischen Verfahren bzw. die verwendeten Verfahren zur Prüfsummenbildung die entsprechende kryptographische Sicherheit gewährleisten.

Stimmen die erste kryptographische Prüfsumme KP1 und die zweite kryptographische Prüfsumme KP2 nicht miteinander überein, so würde die Integrität der Datensegmente Di verletzt und es wird eine Manipulation der Daten festgestellt und vorzugsweise einem Benutzer des Systems gemeldet.

Die Protokolldateneinheiten PDU (Protocol Data Units) sind in SNMP derart aufgebaut, daß in der Nutzdateninformation (sog. Variable Bindings) eine Liste von Objekten (Objektidentikatoren, OID/Value-Pairs) enthalten sein kann. Die Reihenfolge der Objekte innerhalb einer PDU ist dabei nicht festgelegt, so daß eine Permutation der Objekte bei der Übertragung der PDUs zwischen der ersten Anordnung A1 und der zweiten Anordnung A2 auftreten kann. Durch die Erfindung wird es nunmehr möglich, über alle Objekte einer SNMP-PDU eine einzige kryptographische Prüfsumme zu bilden, ohne daß die Reihenfolge der Objekte bzw. der PDUs berücksichtigt werden muß.

Im weiteren werden Alternativen zu dem oben beschriebenen Ausführungsbeispiel erläutert.

Das Verfahren zur Bildung der Prüfsumme PSF kann beispielsweise ein Verfahren zur Bildung von Hashwerten sein. Es kann aber auch Verfahren zur Bildung zyklischer Codes (Cyclic-Redundancy-Check, CRC) unter Verwendung rückgekoppelter Schieberegister eingesetzt werden. Auch können kryptographische Einwegfunktionen zur Bildung der Prüfsummen PSi bzw. PSj verwendet werden.

Im Rahmen dieses Dokuments wurden folgende Veröffentlichungen zitiert:

[1] W. Stallings, Sicherheit in Netzwerk und Internet, Prentice Hall, ISBN 3-930436-29-9, S. 203-223, 1995

[2] K.-H. Kiyek und F. Schwarz, Mathmatik für Informatiker, Teubner Verlag, ISBN 3-519-03277-X, S. 11-13, 1989

d) bei dem durch eine kommutative Verknüpfung (⊕) der zweiten Segmentprüfsummen (Psj) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und

e) bei dem die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, bei dem die Segmentprüfsummen (Psi, Psj) nach mindestens einer der folgenden Arten gebildet werden:
- Hashwertbildung,
- Bildung von CRC-Codes,
- Verwendung mindestens einer kryptographischen Einwegfunktion.

5. Verfahren nach einem der Ansprüche 1 bis 4, bei dem die erste kommutative Prüfsumme (KP1) unter Verwendung mindestens einer kryptographischen Operation kryptographisch gesichert wird.

6. Verfahren nach Anspruch 5, bei dem die kryptographische Operation ein symmetrisches kryptographisches Verfahren ist.

7. Verfahren nach Anspruch 5, bei dem die kryptographische Operation ein asymmetrisches kryptographisches Verfahren ist.

8. Verfahren nach einem der Ansprüche 1 bis 7, bei dem die kommutative Verknüpfung (⊕) die Eigenschaft der Assoziativität aufweist.

9. Verfahren nach einem der Ansprüche 1 bis 8, bei dem digitale Daten gesichert werden, deren Datensegmente (Di) nicht an eine Reihenfolge gebunden sind.

c) für jedes Datensegment (Dj, j = a .. z) der digitalen Daten, denen die erste kommutative Prüfsumme (KP1) zugeordnet ist, eine zweite Segmentprüfsumme (PSj) gebildet wird,
d) durch eine kommutative Verknüpfung (⊕) der zweiten Segmentprüfsummen (Psj) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und
e) die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

14. Anordnung nach einem der Ansprüche 11 bis 13,
bei der die Recheneinheit derart eingerichtet ist, daß die Segmentprüfsummen (Psi, Psj) nach mindestens einer der folgenden Arten gebildet werden:
- Hashwertbildung,
- Bildung von CRC-Codes,
- Verwendung mindestens einer kryptographischen Einwegfunktion.

15. Anordnung nach einem der Ansprüche 11 bis 14,
bei der die Recheneinheit derart eingerichtet ist, daß die erste kommutative Prüfsumme (KP1) unter Verwendung mindestens einer kryptographischen Operation kryptographisch gesichert wird.

16. Anordnung nach Anspruch 15,
bei der die Recheneinheit derart eingerichtet ist, daß die kryptographische Operation ein symmetrisches kryptographisches Verfahren ist.

17. Anordnung nach Anspruch 15,
bei der die Recheneinheit derart eingerichtet ist, daß die kryptographische Operation ein asymmetrisches kryptographisches Verfahren ist.

18. Anordnung nach einem der Ansprüche 11 bis 17,

Zusammenfassung

Verfahren und Anordnung zur Bildung und Überprüfung einer Prüfsumme für digitale Daten, die in mehreren Datensegmente gruppiert sind

Es werden Verfahren und Anordnungen zur Bildung einer Prüfsumme und zur Überprüfung einer Prüfsumme für digitale Daten, die in mehrere Datensegmente gruppiert sind, angegeben. Bei dem Verfahren wird für jedes Datensegment eine Prüfsumme gebildet. Die einzelnen Prüfsummen werden unter Verwendung einer kommutativen Verknüpfung zu einer ersten kommutativen Prüfsumme verknüpft. Zur Überprüfung der ersten kommutativen Prüfsumme wird für jedes Datensegment wiederum eine Prüfsumme gebildet und die Prüfsumme wiederum unter Verfahren einer kommutativen Verknüpfung zu einer zweiten kommutativen Prüfsumme verknüpft. Die erste kommutative Prüfsumme und die zweite kommutative Prüfsumme werden auf Übereinstimmung überprüft.